DE GRUYTER
OPEN

TATRA
MOUNTAINS
Mathematical Publications
DOI: 10.1515/tmmp-2017-0021
Tatra Mt. Math. Publ. **70** (2017), 107–117

ON THE FAMILIES OF STABLE MULTIVARIATE TRANSFORMATIONS OF LARGE ORDER AND THEIR CRYPTOGRAPHICAL APPLICATIONS

Vasyl Ustimenko

ABSTRACT. Families of stable cyclic groups of nonlinear polynomial transformations of affine spaces K^n over general commutative ring K of with n increasing order can be used in the key exchange protocols and El Gamal multivariate cryptosystems related to them. We suggest to use high degree of noncommutativity of affine Cremona group and modify multivariate El Gamal algorithm via conjugations of two polynomials of kind g^k and g^{-1} given by key holder (Alice) or giving them as elements of different transformation groups. Recent results on the existence of families of stable transformations of prescribed degree and density and exponential order over finite fields can be used for the implementation of schemes as above with feasible computational complexity.

1. Introduction

Multivariate cryptography [1] is one of the directions of *Post Quantum Cryptography* (PQC). Some examples of multivariate cryptography algorithms can be constructed in terms of algebraic graph theory (see Section 2, which is a brief introduction to this area). Section 3 is devoted to Diffie-Hellman type key exchange algorithm for a cyclic subgroup of affine Cremona group and a related idea of a stable transformation of an affine space over general commutative ring. The basic version of a multivariate ElGamal algorithm is also discussed there, some results on constructions of examples of families of stable transformations are observed. Notice that one can use more general families of transformations of bounded degree and large order instead of stable transformations in protocol and cryptosystem mentioned above. For instance, in the case of finite fields

2010 Mathematics Subject Classification: Primary 11T71; Secondary 11Rxx.
Keywords: Multivariate cryptography, stable transformations, key exchange protocols, shifted multivariate ElGamal algorithm, desynchronisation diagram.
This research is partially supported by the grant PIRSES-GA-2013-612669 of the 7th Framework Programme of European Commission.

one can use classical Singer transformations τ_n of vector spaces ${F_q}^n$ of order $q^n - 1$ (see [2] or [3] and further references) and a family of stable maps g_n of degree d. Then elements of kind $f_n = {g_n}^{-1}\tau_n g_n$ form a family of order $q^n - 1$ and degree bounded by d^2. Notice that inverses of f_n also have degree $\leq d^2$. In the majority of known cases of stable families of g_n mentioned in Section2 one can easily check that related transformations f_n are nonlinear. Such elements can be used as generators of cyclic groups used in multivariate Diffie-Hellman protocols and multivariate ElGamal cryptosystems.

Section 4 is devoted to shifted ElGamal cryptosystem, which uses high level of noncommutativity in affine Cremona group. We also consider more general schemes, where key holder uses desynchronisation process to send conjugates of g^k and g^{-1} as elements of different groups.

2. On Post Quantum and Multivariate Cryptography

Post Quantum Cryptography serves for the research of asymmetrical cryptographical algorithms which can be potentially resistant against attacks based on the use of quantum computer.

The security of currently popular algorithms is based on the complexity of the following three known hard problems: integer factorisation, discrete logarithm problem, discrete logarithm for elliptic curves.

Each of these problems can be solved in polynomial time by Peter Shor's algorithm for theoretical quantum computer.

Despite the fact that the known small experimental examples of quantum computer are nowadays not able to attack currently used cryptographical algorithms, cryptographers have already started the research on postquantum security. They should also mind new results of general complexity theory such as complexity estimations of isomorphism problem obtained by L. Babai [4].

The history of international conferences on Post Quantum Cryptography (PQC) started in 2006.

We have to notice that Post Quantum Cryptography differs from Quantum Cryptography, which is based on the idea of using quantum phenomena to reach better security.

Modern PQC is divided into several directions such as:

- Multivariate Cryptography,
- Lattice based Cryptography,
- Hash based Cryptography,
- Code based Cryptography, and
- studies of isogenies for superelliptic curves.

The oldest direction is Multivariate Cryptography which uses polynomial maps of affine space K^n defined over a finite commutative ring K into itself as encryption tools. It exploits the complexity of finding a solution of a system of nonlinear equations with many variables. Multivariate cryptography uses as security tools nonlinear polynomial transformations of kind:

$$x_1 \to f_1(x_1, x_2, \dots, x_n), \quad x_2 \to f_2(x_1, x_2, \dots, x_n), \dots, \quad x_n \to f_n(x_1, x_2, \dots, x_n)$$

acting on the affine space K^n, where

$$f_i \in K[x_1, x_2, \dots, x_n], \quad i = 1, 2, \dots, n$$

are multivariate polynomials given in a standard form, i. e., via a list of monomials in chosen order. The reader can find important ideas in this direction in ([6], [7], [8]).

The current task is a search for an algorithm resistant to cryptoanalytic attacks based on an ordinary Turing machine. Multivariate cryptography has to demonstrate a practical security algorithm, which can compete with RSA, Diffie--Hellman protocols, popular methods of elliptic curve cryptography (see [1], [9]).

This is still a young promising research area with the current lack of known cryptosystems with the proven resistance against attacks with the use of ordinary Turing machines. Studies of attacks based on Turing machines and quantum computers have to be investigated separately because of different natures of the two machines, deterministic and probabilistic, respectively.

Recall that K stands for a commutative ring. Symbol $S(K^n)$ stands for the affine Cremona semigroup of all polynomial transformations of affine space K^n.

Multivariate cryptography started from the studies of potential candidates for the special quadratic encryption multivariate bijective map of K^n, where K is an extension of finite field F_q of characteristic 2. One of the first such cryptosystems was proposed by Imai and Matsumoto, cryptanalysis for this system was invented by J. Patarin. The survey on various modifications of this algorithm and corresponding cryptanalysis can be found in [1]. Various attempts to build secure multivariate public keys were unsuccessful, but the research of the development of new candidates for secure multivariate public keys is going on (see, for instance, [10] and further references).

Applications of Algebraic Graph Theory to Multivariate Cryptography were recently observed in [11]. This survey is devoted to algorithms based on bijective maps of affine spaces into themselves. Applications of algebraic graphs to cryptography started with symmetric algorithms based on explicit constructions of extremal graph theory and their direct analogue. The main idea is to convert an algebraic graph to a finite automaton and to use the pseudorandom walks on the graph as encryption tools. This approach can be also used for the key exchange protocols. Nowadays, the idea of "symbolic walks" on algebraic graphs, when a walk on a graph depends on parameters given as special multivariate polynomials in variables depending of the plainspace vector, is used in several public key cryptosystems. Other source of graphs suitable for cryptography is connected with finite geometries and their flag system (see [11] and further references). Bijective multivariate sparse encryption maps of a rather high degree based on walks in algebraic graphs were proposed in [12].

One of the first usage of a non-bijective map of multivariate cryptography was in *oil and vinegar* cryptosystem analysed in [5]. The observations of further research on non-bijective multivariate cryptography can be found in [19] (proceedings of the International Conference DIMA 2015 in Belarus), where the new cryptosystem with non-bijective multivariate encryption maps on the affine space ${Z_m}^n$ into itself was presented together with some results concerning the construction of bijective stable transformations of large order of finite vector spaces. The technique of [13] is based on the usage of the embeddings of projective geometries into corresponding Lie algebra (see [25] and further references).

3. On stable multivariate transformations for the key exchange protocols

It is widely known that Diffie-Hellman key exchange protocol can be formally considered for the generator g of a finite group or semigroup G. Users need a large set $\{g^k | k = 1, 2, \dots\}$ to make it practical. One can see that the security of the method depends not only on the abstract group or semigroup G, but also on its representation. If G is a multiplicative group F_p^* of finite field F_p, then we have a case of classical Diffie-Hellman algorithm. If we change ${F_p}^*$ to isomorphic group Z_{p-1}, then the security will be completely lost. We have a problem of solving a linear equation instead of a discrete logarithm problem to measure the security level.

Let K be a commutative ring. $S(K^n)$ stands for the Cremona affine semigroup of all polynomial transformations of the affine space K^n. Let us consider a multivariate Diffie-Hellman key exchange algorithm for the generator $g(n)$ semigroup G_n of affine Cremona semigroup.

Correspondents (Alice and Bob) agree on this generator$g(n)$ of the group of type:

$$x_1 \to f_1(x_1, x_2, \dots, x_n),$$
$$x_2 \to f_2(x_1, x_2, \dots, x_n), \dots,$$
$$x_n \to f_n(x_1, x_2, \dots, x_n)$$

acting on the affine space K^n, where

$$f_i \in K[x_1, x_2, \dots, x_n], \quad i = 1, 2, \dots, n \quad \text{are multivariate polynomials.}$$

Alice chooses a positive integer k_A as her private key and computes the transformation $g(n)^{k_A}$ (multiple iterations of $g(n)$ with itself).

Similarly, Bob chooses k_B and gets $g(n)^{k_B}$. Correspondents complete the exchange: Alice sends $g(n)^{k_A}$ to Bob and receives $g(n)^{k_B}$ back from him. Now Alice and Bob computes independently common key h as

$$\left(g(n)^{k_B}\right)^{k_A} \quad \text{and} \quad \left(g(n)^{k_A}\right)^{k_B}, \quad \text{respectively.}$$

So they can use the coefficients of the multivariate map $h = g(n)^{k_B k_A}$ from G_n written in the standard form.

There are obvious problems preventing the implementation of this general method in practice. In case $n = 1$ the degree $\deg(fg)$ of composition fg of elements $f, g \in S(K)$ is simply the product of $\deg(f)$ and $\deg(g)$. Such an effect can happen in the multidimensional case: $(\deg(g))^x) = \deg(g^x) = b$. It causes the reduction of discrete logarithm problem for multivariate polynomials to a number theoretical problem. If g is a bijection of degree d and order m, then $d^x = b$ in cyclic group Z_m. Similar reduction can appear in the case of other degree functions $s(x) = \deg(g^x)$. If $s(x)$ is a linear function, then multivariate discrete logarithm problem with base g is reducible to the solution of a linear equation. The degenerate case $\deg(g^x) = \mathit{const}$ is an interesting one because in such situation the degree function does not help to investigate the multivariate discrete logarithm.

We refer to the sequence of multivariate transformations $f(n) \in S(K^n)$ as stable maps of degree d if $\deg(f(n))$ is a constant $d, d > 2$ and $\deg(f(n)^k) \leq d$ for $k = 1, 2, \ldots$ (see [15]). If τ_n is a bijective affine transformation of K^n, i. e., a bijective transformation of degree 1, then the sequence of stable maps $f(n)$ can be changed to another sequence of stable maps $\tau f(n) \tau^{-1}$ of the same degree d.

The first families of special bijective transformations of K^n of bounded degree were generated by *discrete dynamical systems* defined in [14] in terms of graphs $D(n, K)$. The fact that each transformation from these families of maps is cubic was proven in the paper [16]. In [15] authors notice that this family is stable, the order of its members grows with the increase of parameter n and suggest key exchange protocols with generators from these families. In fact, graphs $D(n, K)$ were introduced in [17] in a connection to their cryptographical applications. Graphs $D(n, q) = D(n, F_q)$ had appeared even earlier [18], [19] in a connection to their applications to extremal combinatorics.

Another example of stable families of cubic transformations over general commutative ring K is associated with the dynamical systems of other family of algebraic graphs $A(n, K)$ (see [20] and further references). The family of quadratic stable transformations of K^n, were introduced in [21], the order of the maps is not yet evaluated.

Recall that the other important property of the generator $g(n)$ in the protocol described above is a large cardinality of $\{g(n)^k | k = 1, 2, \dots\}$. Let us assume that $g(n)$ are bijections. We say that $g(n)$ is a family of exponential order if the order $|g(n)|$ is at least $a^{\alpha n}$, where $a > 1$ and $\alpha > 0$ are constants. The famous family of linear bijections over F_q of exponential order is formed by Singer cycles $s(n)$, they have order $q^n - 1$.

As it was mentioned in the Introduction, we can use Singer cycles for a creation of nonlinear families of exponential growth, which can serve as bases for the key exchange protocols described above in the following way. We say that a family of nonlinear transformations $f(n)$ of affine space K^n is the family of strongly bounded degree, if degrees of all functions $f(n)^k$, $k = 1, 2, \dots$ are bounded above by constant d. It is easy to see that a class of such families is slightly wider than a class of stable transformations. Let $g(n)$ be a family of bijective stable transformations of ${F_q}^n$ of degree t, then ${g(n)}^{-1}s(n)g(n)$ is a family of exponential order $(q^n - 1)$ and strongly bounded degree (bounded above by t^2).

The above key exchange protocol can be used to design the following multivariate ElGamal cryptosystem (see [22]). Alice takes generator $g(n)$ of the group G_n together with its inverse $g(n)^{-1}$. She sends the pair $\big(g(n), g(n)^{-1}\big)$ to Bob. He will work with the plainspace K^n as a public user.

At the beginning of each session

- Alice chooses her private key k_A. She computes $f = g(n)^{k_A}$ and sends it to Bob.
- Bob writes his text $(p_1, p_2, \dots, p_n)$, chooses his private key k_B and creates the ciphertext $f^{k_B}\big((p_1, p_2, \dots, p_n)\big) = \mathrm{c}$.
- Additionally he computes the map ${g(n)^{-1}}^{k_B} = h(n)$.
- He sends the pair $(c_1, c_2, \dots, c_n), h(n)$ to Alice.
- Alice computes ${h(n)}^{k_A}(\mathrm{c}) = (p_1, p_2, \dots, p_n)$.

Remark 1. It is proven (see [22]) that the security level of the above multivariate Diffie-Hellman and ElGamal algorithms is the same. It is based on the multivariate discrete logarithm problem.

Solve the equation $g^x = d$, where g and d are elements of special cyclic subgroup G_n of affine Cremona group.

Remark 2. It is clear that the algorithm above can be formally considered for the general pair of bijective nonlinear polynomial transformations $g(n)$ and $g(n)^{-1}$ of free module K^n. For computational feasibility, we will require that $g(n)$ has to be a family of strongly bounded degree. Obviously parameter $|G_n|$ has to grow with the increase of n.

4. On the shifted multivariate ElGamal cryptosystem

4.1. On the usage of noncommutativity of affine Cremona group

We say that family of elements $h(n) \in C(K^n)$ of affine Cremona group is of symmetrical bounded degree if sequences $\deg h(n)$ and $\deg h^{-1}(n)$ are bounded by some independent constant.

We refer to a family $g(n) \in C(K^n)$ as a family of strictly bounded degree if integers $\deg g^k(n)$ are bounded by a number independent from n and k constants.

We suggested at CECC 2016 the following modification of the algorithm described in the previous section. Assume that Alice takes the family of generators $g(n)$ of cyclic groups G_n of large order with its inverse $g(n)^{-1}$ and it is a family of strictly bounded degree. Two other families $h_1(n)$ and $h_2(n)$ are families of symmetrically bounded degrees and the sequences of

$$h_1{}^{-1}(n) \quad \text{and} \quad h_2{}^{-1}(n) \quad \text{are computable for Alice.}$$

1) Alice chooses large positive integer k_A as her private key.
2) After that she computes $R(n) = g(n)^{k_A} \in C(K^n)$ and its conjugation $Q(n) = h_1(n)R(n)h_1{}^{-1}$.
3) Alice computes the transformation $H(n) = h_2(n)g(n)^{-1}h_2(n)^{-1}$.
   She sends $G(n)$ and $H(n)$ to Bob.

— Bob chooses his private key k_B, writes his plaintext $\mathrm{p}=(p_1, p_2, \dots, p_n)$,

— computes $H^{k_B}(n)$ and the ciphertext $\mathrm{c} = Q^{k_B}(n)(\mathrm{p})$ via multiple application (k_B times) of $Q(n)$ to the tuple from K^n.

— Bob sends vector c to Alice together with $H' = H^{k_B}$.

Alice decrypts via the following steps:

1. She computes g^{-k_B} as $h_2{}^{-1}(n)H'(n)h_2(n)$.
   Really, $h_2{}^{-1}H'h_2 = h_2{}^{-1}(h_2 g^{-k_B} h_2{}^{-1})h_2$.
2. Alice creates $H_1 = h_1 g^{-k_B} h_1{}^{-1}$.
3. She applies k_A times H_1 to ciphertext and computes the plaintext.
   In fact, $H_1^{k_A}(\mathrm{c}) = \mathrm{p}$.

The shifted algorithm may have better protection against attacks by an adversary. One can choose $h_2(n)$ to make the discrete logarithm problem in affine Cremona group with the new base $H(n)$ harder than one in a case of base $g(n)^{-1}$. Additionally, the adversary has to compute the inverse of $Q(n)$.

Remark 1. Alice can work with a stable map $g(n)$ of a large order.

4.2. ElGamal desynchronisation diagram

Let G be a group acting on a set M. ElGamal algorithm for this situation with the plainspace M is suggested in [23].

Below, we consider more general cryptosystem defined over the diagram

$$S(M) \leftarrow G'_1 \leftarrow G_1 \leftarrow G \rightarrow G_2 \rightarrow G'_2.$$

The left node of the diagram is a symmetric group $S(M)$ of all permutations on the set M, link $G'_1 \leftarrow G_1$ corresponds to homomorphism η_1 of group G_1 into group G'_1, the link $G'_1 \rightarrow S(M)$ corresponds to homomorphism δ of group G'_1 into $S(M)$. So group G'_1 acts on the set M. Links $G_1 \leftarrow G$ and $G \rightarrow G_2$ correspond to embeddings ϕ_1 and ϕ_2 of the group G into groups G_1 and G_2, link $G_2 \rightarrow G'_2$ corresponds to homomorphism of G_2 into group G'_2.

We assume that for kernel H_2 of the map η_2 of G_2 into G'_2 the condition

$$|\phi_2(G) \cap H_2| = 1 \quad \text{holds.}$$

We refer to these data as a desynchronisation ElGamal diagram.

We propose the following cryptosystems:

- Alice generates the pair g, g^{-1} of elements of G. She chooses integer parameter $k_A > 1$ and computes g^{k_A} and elements $g_A = h_1 g^{k_A} {h_1}^{-1}$ for selected $h_1 \in G$, takes $\phi_1(g_A)$ and its conjugation $g_1\phi_1(g_A){g_1}^{-1}$ for $g_1 \in G_1$.
- After that she computes
$$\eta_1(g_1)\phi_1(g_A){g_1}^{-1} \quad \text{and} \quad h'_1\Big(\eta_1\big(g_1\phi_1(g_A){g_1}^{-1}\big)\Big){h'_1}^{-1} = h_A$$
for certain $h'_1 \in G'_1$.
- Finally, she takes $\delta(h_A)$ and $\pi \in S(M)$ and creates $\pi(\delta(h_A)\pi^{-1} = \pi_A$.
- Additionally, Alice takes g^{-1} forms $h_2 g^{-1} {h_2}^{-1}$ for selected $h_2 \in G$.
She computes $\phi_2(h_2 g^{-1} {h_2}^{-1})$ and $h'_2\phi_2(h_2 g^{-1} {h_2}^{-1}){h'_2}^{-1} = s$ for selected $h'_2 \in G_2$. She forms $\eta_2(s)$ and $s' = t\eta_2(s)t^{-1}$ for chosen parameter $t \in G'_2$.
- Alice sends π_A and s' to Bob.

— Bob picks up parameter k_B and writes message m. He applies k_B times parameter π_A to m, forms ciphertext ${\pi_A}^{k_B}(m) = c$ and sends it to Alice together with element ${s'}^{k_B}$ of group G'_2.

Alice uses the following decryption algorithm:

- She takes map ${s'}^{k_B}$ and computes $t^{-1}{s'}^{k_B}t = \eta_2(s)^{k_B} = \eta_2(s^{k_B})$. Thus $\eta_2\big(h'_2\phi_2(h_2 g^{-k_B} {h_2}^{-1})({h'_2}^{-1})\big) = \eta_2(s^{k_B})$.
- Alice computes
$$\phi_2\big(h_2 g^{-k_B} {h_2}^{-1}\big) \quad \text{as} \quad \eta_2(h'_2)^{-1}\eta_2(s^{k_B})\eta_2(h'_2).$$

Notice, that $r = h_2 g^{-k_B} {h_2}^{-1}$ is an element of G and the condition on H_2 allows to compute Alice element r and g^{-k_B}.

After that Alice computes $(g^{-k_B})^{k_A} = d$ and takes consecutively

$$\phi_1(d), \quad \eta_1\big(\phi_1(d)\big) \quad \text{and} \quad \delta\Big(\eta_1\big(\phi_1(d)\big)\Big) = \tau.$$

So, she obtains the plaintext as $\tau(c)$.

Example. Let us consider the embeddings of finite fields F_q into its extensions F_{q^m} and F_{q^k}. They induce embeddings η_1 and η_2 of the general linear group $GL(n,q)$ into $GL(n, F_{q^m})$ and $GL(n, F_{q^k})$ which are subgroups of Affine Cremona Groups

$$C_1 = C({F_{q^m}}^n) \quad \text{and} \quad C_2 = C({F_{q^k}}^n)\,.$$

Alice takes Singer cycle g_n of group $GL(n, F_q)$ of order $q^n - 1$. She forms $\eta_1(g_n)$, takes elements $h_n \in Gl(n, F_{q^m})$ and stable transformation $\pi_1 \in C_1$ of degree d_1. She takes her private key k_A (positive integer) and forms element

$$\pi_1 h_n {g_n}^{k_A} {h_n}^{-1} {\pi_1}^{-1} = F_n.$$

Notice that $F_n \in C_1$. Alice writes this map in a standard form

$$x_i \to f_i, \quad f_i \in F_{q^m}[x_1, x_2, \ldots, x_n], \quad i = 1, 2, \ldots, n$$

and creates $G_n = \pi_2 l_n {g_n}^{-1} {l_n}^{-1} {\pi_2}^{-1}$ written in a standard form

$$x_i \to g_i, \quad g_i \in F_{q^k}[x_1, x_2, \ldots, x_n], \quad i = 1, 2, \ldots, n\,.$$

Bob writes a message $\mathrm{p} = (p_1, p_2, \ldots, p_n) \in F_{q^m}$. He chooses a private key k_B for the creation of his ciphertext c via application of a map F, exactly, k_B times to p. Bob computes element $H = {G_n}^{k_B}$ of Affine Cremona Group C_2 and sends pair H, $\mathrm{c} = F^{k_B}(\mathrm{p})$.

For decryption, Alice computes conjugates ${g_n}^{-k_B}$ of H. The knowledge of L_n and π_2 allows her to do this step. Secondly, Alice forms $Q = \pi_1 h_n {g_n}^{-k_B} {h_n}^{-1} \pi_1^{-1}$. She applies Q to c exactly k_A times and gets the plaintext.

Remark 1. We can modify the above algorithm by changing C_1 and C_2 for Affine Cremona Groups

$$C_1' = C({F_q}^{nm}) \quad \text{and} \quad C_2' = C({F_q}^{nk}).$$

So Alice takes $h_n \in GL(nm, F_q)$, $l_n \in GL(nk, F_q)$, $\pi_1 \in C_1'$ and $\pi_2 \in C_2'$. So the standard form of F and G are

$$x_i \to f_i, \quad f_i \in F_q[x_1, x_2, \ldots, x_{nm}], \quad i = 1, 2, \ldots, nm$$

and

$$x_i \to g_i, \quad f_i \in F_q[x_1, x_2, \ldots, x_{n\,k}], \quad i = 1, 2, \ldots, nk.$$

Remark 2. Let us assume that $q = p^s$, $s \geq 2$. Then C_1 and C_2 can be changed for symmetric groups $S_{p^{nms}}$ and $S_{p^{nks}}$. The Singer cycle g_n can be taken from $GL(ns, F_p)$. So Alice takes

$$h_n \in GL(nms, F_p), l_n \in GL(nks, F_p), \pi_1 \in S_{p^{nms}} \quad \text{and} \quad \pi_2 \in S_{p^{nks}}$$

So the standard form of F and G are

$$x_i \to f_i, \quad f_i \in F_q[x_1, x_2, \ldots, x_{nms}], \quad i = 1, 2, \ldots, nms$$

and

$$x_i \to g_i, \quad f_i \in F_q[x_1, x_2, \ldots, x_{nks}], \quad i = 1, 2, \ldots, nks.$$

Remark 3. Graphs-based constructions of quadratic and cubic stable transformations of affine space K^n over general commutative degree are observed in Section 3. Methods of a construction of a stable transformation of K^n of a fixed prescribed degree based on graphs $D(n, K)$ are presented in [24].

REFERENCES

[1] DING, J.—GOWER, V.—SCHMIDT, D. S.: *Multivariate Public Key Cryptosystems*. In: Adv. Inform. Sec. Vol. 25, Springer-Verlag, New York, 2006.

[2] COSSIDENTE, A.—DE RESMINI, M. J.: *Remarks on Singer cyclic groups and their normalizers*, Des. Codes Cryptogr. **32** (2004), no. 1–3, 97–102,

[3] KANTOR, W.: *Linear groups containing a Singer cycle*, J. Algebra **62** (1980), no. 1, 232–234.

[4] BABAI, L.: *Graph isomorphism in quasipolinomial time*, arXive: 1512 03547v1 [cs. DS], December 11, 2015.

[5] KIPNIS, A.—SHAMIR, A.: *Cryptanalisis of the Oil and Vinegar Signature Scheme*, Adv. in Cryptology—Crypto '96, Lect. Notes in Comput. Sci. Vol. 1462, 1996, pp. 257–266.

[6] PATARIN, J.—GOUBIN, L.: *Trapdoor one-way permutations and multivariate polynominals*, ICICS 1997, pp. 356–368.

[7] ______ *Asymmetric cryptography with S-Boxes*, ICICS 1997, pp. 369–380.

[8] PATARIN, J.: *Asymmetric cryptography with a hidden monomial, and a candidate algorithm for $\simeq$ 64 bits asymmetric signatures*. In: Advances in cryptologyCRYPTO '96, Santa Barbara, CA), Lect. Notes in Comput. Sci. Vol. 1109, Springer-Verlag, Berlin, 1996, pp. 45–60.

[9] GOUBIN, L.—PATARIN, J.—YANG, B.-Y.: *Multivariate Cryptography*. Encyclopedia of Cryptography and Security (2nd ed.), Springer-Verlag Berlin 2011, pp. 824–828.

[10] PORRAS, J.—BAENA, J.—DING, J.: *New candidates for multivariate trapdoor functions*, Rev. Colombiana Mat. **49** (2015), no. 1, 57–76.

[11] USTIMENKO, V. A.: *Explicit constructions of extremal graphs and new multivariate cryptosystems*, In: Proceedings of The Central European Conference, 2014, Budapest", Studia Sci. Math. Hungar. **52** (2015), 185–204.

[12] ______ *On multivariate cryptosystems based on computable maps with invertible decompositions*, Ann. Univ. Mariae Curie-Skłodowska Sect. AI-Inform. **14** (2014), 7–18.

[13] ______ *On Shubert cells in grassmanians and new algorithm of multivariatecryptography*, Tr. Inst. Mat. **23** (2015), no. 2, 137–148

[14] ______ *On Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Zap. Nauchn. Semin. POMI **326**, (2005), 214–234; translated in J. Math. Sci., **140** (2007), no. 3, 461–471.

[15] USTIMENKO, V.—WROBLEWSKA, A.: *On the key exchange with nonlinear polynomial maps of stable degree*, Ann. Univ. Mariae Curie-Skodowska Sect. AI-Inform. **13** (2013), no. 1, 63–80.

[16] WROBLEWSKA, A.: *On some properties of graph based public keys*, Albanian J. Math. **2** (2008), no. 3, 229–234.

[17] USTIMENKO, V.: *Coordinatisation of trees and their quotients.* In: the "Voronoj's Impact on Modern Science", Vol 2, 1998, Kiev, Institute of Mathematics pp. 125–152.

[18] LAZEBNIK, F.—USTIMENKO, V. A.: *Some algebraic constractions of dense graphs of large girth and of large size.* In: Expanding graphs, Princeton, NJ, 1992, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Vol. 10, 1993, Amer. Math. Soc., Providence, RI, pp. 75–93.

[19] LAZEBNIK, F.—USTIMENKO, V. A. —WOLDAR, A. J.: *New series of dense graphs of high girth*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), no. 1, 73–79.

[20] USTIMENKO, V.— ROMANCZUK, U.: *On dynamical systems of large girth or cycle indicator and their applications to multivariate cryptography.* In: Artificial Intelligence, Evolutionary Computing and Metaheuristics, In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer-Verlag, 2013, pp. 257—285.

[21] USTIMENKO, V.—WROBLEWSKA, A.: *Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography*, Ann. Univ. Mariae Curie-Skodowska Sect. AI-Inform. **12** (2012), no. 3, 65–74.

[22] KLISOWSKI, M.: *Zwięszenie Bezpieczeństwa Kryptograficznych Algorytmówielu Zmiennych Bazujących na Algebraicznej Teorii Grafów.* PhD Thesis, Częstochowa, 2014.

[23] KLISOWSKI, M.—USTIMENKO, V.: *Graph based cubical multivariate maps and their cryptographical applications.* In: Advances on Superelliptic curves and their Applications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., Vol. 41, IOS, Amsterdam, 2015 pp. 305–327.

[24] WROBLEWSKA, A.—USTIMENKO, V.: *On new examples of families of multivariate stable maps and their cryptographical applications*, Ann. Univ. Mariae Curie-Skłodowska Sect. AI-Inform. **14** (2014), no. 1, 19–35.

[25] , USTIMENKO, V.— WOLDAR, A.: *A geometric approach to orbital recognition in Chevalley-type coherent configurations and association schemes*, Australas. J. Combin. **67** (2017), no. 2, 166–202.

Received August 13, 2017

Faculty of Mathematics,
Physics and Computer Science
Maria Curie-Skłodowska University
Plac Marii Curie-Skłodowskiej 1
PL-20-031 Lublin
POLAND
E-mail: vasyl@hektor.umcs.lublin.pl